



# UNITED STATES PATENT AND TRADEMARK OFFICE

mn

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.   | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.            | CONFIRMATION NO.       |
|---|-------------|----------------------|--------------------------------|------------------------|
| 10/028,382  | 12/21/2001  | Michael A. Epstein   | US010632                       | 4889                   |
| 24737 7590 06/08/2007<br>PHILIPS INTELLECTUAL PROPERTY & STANDARDS<br>P.O. BOX 3001<br>BRIARCLIFF MANOR, NY 10510 |             |                      | EXAMINER<br>PYZOCHA, MICHAEL J |                        |
|   |             |                      | ART UNIT<br>2137               | PAPER NUMBER           |
|   |             |                      | MAIL DATE<br>06/08/2007        | DELIVERY MODE<br>PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

**MAILED**

**JUN 08 2007**

**Technology Center 2100**

Application Number: 10/028,382  
Filing Date: December 21, 2001  
Appellant(s): EPSTEIN, MICHAEL A.

William S. Francos  
(Reg. No. 38,456)  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 02/05/2007  
appealing from the Office action mailed 07/07/2006.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

Art Unit: 2137

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

|            |                |         |
|------------|----------------|---------|
| 5907619    | DAVIS          | 5-1999  |
| EP 1041767 | AKIYAMA et al. | 10-2000 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

**Claim Rejections - 35 USC § 102**

Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Akiyama, European Patent Application No. EP 1,041,767.

As per claims 1 and 4, the applicant describes a hashing system with the following limitation which is met by Akiyama: a) a plurality of hash devices ([0029]); b) each hash device of the plurality of hash devices being configured to receive a sequence of data values and apply a hash function to the received subset of the sequence of data values when enabled, said hash function being the same in said each hash device ([0029], [0050], Fig 1, Fig 3A); c) at least one comparator, operably coupled to the plurality of hash devices, that is configured to compare an output of each hash device to the source hash value, to

Art Unit: 2137

facilitate a verification of the sequence of data values ([0030], Fig 1).

As per claims 2 and 5, the applicant describes the hashing system of claims 1 and 4, which are met by Akiyama, with the following limitation which is also met by Akiyama: Wherein each hash device is enabled sequentially ([0062], Fig 4B).

As per claims 3 and 6, the applicant describes the hashing system of claims 1 and 4, which are met by Akiyama, with the following limitations which are also met by Akiyama: a) said each hash device is enabled to receive and process K data values (Fig 4A, Fig 4B); b) the plurality of hash devices corresponds to K hash devices (Fig 4A, Fig 4B).

Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent No. 5,907,619.

As per claims 1 and 4, the applicant describes a hashing system with the following limitation which is met by Davis: a) a plurality of hash devices (Col 5, lines 21-28; Fig 3); b) each hash device of the plurality of hash devices being configured to receive a sequence of data values and apply a hash function to the received subset of the sequence of data values when enabled, said hash function being the same in said each hash device (Col 5, lines 21-28; Fig 3); c) at least one comparator, operably

Art Unit: 2137

coupled to the plurality of hash devices, that is configured to compare an output of each hash device to the source hash value, to facilitate a verification of the sequence of data values (Col 5, lines 21-28; Fig 3).

As per claims 2 and 5, the applicant describes the hashing system of claims 1 and 4, which are met by Davis, with the following limitation which is also met by Davis: Wherein each hash device is enabled sequentially (Col 5, lines 21-28; Fig 3).

As per claims 3 and 6, the applicant describes the hashing system of claims 1 and 4, which are met by Davis, with the following limitations which are also met by Davis: a) said each hash device is enabled to receive and process K data values (Col 5, lines 21-28; Fig 3); b) the plurality of hash devices corresponds to K hash devices (Col 5, lines 21-28; Fig 3).

#### **(10) Response to Argument**

I. Rejection of claims 1-6 rejected under 35 USC 102(b) in view of Akiyama.

Appellant argues that Akiyama does not disclose that the hash function is the same in each hash device.

With respect to this argument Appellant is directed to Figures 2A and 2B. Specifically in Figure 2A the one-way function 22 is used in each of the n hashing steps and that "each of the hash units 2 consists of an EOR 21, a one-way

Art Unit: 2137

function 22 such as a hash function, and a truncator 23."

Furthermore paragraph [0045] describes, in more detail, the steps being performed in Figures 2A and 2B, "the one-way function 22 performs a one-way operation (e.g. an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain the value L11".

Appellant is also directed to paragraph [0040] where Akiyama states that the one-way function 22 is a one-way function device, which creates the authenticators with the one-way function operation (the operation as described in paragraph [0045]). In paragraph [0034] Akiyama discloses "authenticators are created with a different key for each of the data D1 to Dn" which shows that the different keys used with the one-way function 22 are what make the different one-way functions mentioned in paragraph [0014]. This is because the one-way functions mentioned in paragraph [0014] are the devices described in paragraph [0040] and the different keys used with the one-way function operations within the devices are what differentiate the one-way function devices. Therefore the one-way function operations are the same in each one-way function 22.

II. Rejection of claims 1-6 rejected under 35 USC 102(b) in view of Davis.

Art Unit: 2137

Appellant argues that Davis does not disclose that the hash function is the same in each hash device.

Appellant specifically argues that since Davis teaches, "Different hashing functions may be used" Davis does not teach that the hashing functions are the same. However since Davis teaches that "Different hashing functions **may be** used" (emphasis added) Davis also teaches that different hashing functions may not be used, i.e. using the same hashing functions. In other words the situation when different hashing functions are used is an alternative embodiment and the main embodiment uses the same hashing function. Therefore, Davis teaches the hash functions are the same in each hash device.

**(11) Related Proceeding(s) Appendix**


No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.



Art Unit: 2137

For the above reasons, it is believed that the rejections should be sustained.

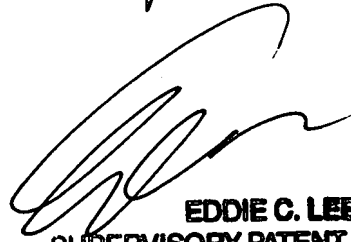
Respectfully submitted,

Michael J. Pyzocha 

June 5, 2007

Conferees:

Eddie Lee

  
**EDDIE C. LEE**  
**SUPERVISORY PATENT EXAMINER**

Emmanuel Moise 